TAMMIS-MEDREG

Theater Army Medical Management Information System – Medical Regulating

Questions or comments related to this plan should be directed to:

Contingency Plan Point of Contact:
Major Craig Anderson
Organization: USAMISSA
Phone: 210-221-1300
Email: craig.anderson@amedd.army.mil

US ARMY MEDICAL DEPARTMENT

AMEDD Year 2000 Contingency and Continuity of Operations Plan

FOR

TAMMIS PATIENT SYSTEMS (MEDREG)

US ARMY MEDICAL INFORMATION SYSTEMS AND SERVICES AGENCY (USAMISSA)
THEATER ARMY MEDICAL MANAGEMENT INFORMATION SYSTEM
SAN ANTONIO, TEXAS 78217

1 APRIL 1999

Executive Summary

This TAMMIS MEDREG Year 2000 (Y2K) Continuity of Operations Plan (COOP) is written to help ensure the MEDREG system is not adversely effected by year 2000 events. Year 2000 problems stem from the practice of using two digits instead of four digits ("99" vs "1999") to represent the year, resulting in the inability of computers and devices to interpret Year 2000 dates as greater than 1900 dates. This problem is compounded by the fact that corrupted data can be perpetuated through interfaces to other information systems.

The TAMMIS system project office, USAMISSA, has prepared this COOP in response to an AMEDD/HA request, and to protect mission capability. This COOP was developed as a stand-alone document because there is no existing COOP that can be modified to address Y2K events.

This COOP has been developed per guidance contained in the DoD MHS Year 2000 Contingency and Continuity of Operations Planning Guide.

This COOP covers only the MEDREG system.

MEDREG is a mission essential system. This plan addresses all phases of the MEDREG mission. Y2K contingency planning activities contained in Appendix D are prioritized based on their probability of occurrence and their potential impact to the MEDREG mission.

Risk mitigation efforts for Computer Systems, Communication Systems, Data Collection and Analysis Tools have been addressed as they apply to the MEDREG system and are included as annexes. Besides having a plan available to execute if Y2K events adversely impact MEDREG mission capability, one of the major benefits of developing this COOP has been the exercise of identifying essential sub-systems and work-around required to protect Patient Administration mission capabilities. This plan will continue to evolve as we gain more knowledge of potential Y2K event impacts.

Table of Contents

Introduction/Purpose

The purpose of this plan is to provide Year 2000 (Y2K) contingency planning information to all AMEDD (MEDREG) System personnel in the event that the MEDREG systems or processes are adversely impacted during the transition to the year 2000. It applies to all TO&E units that have MEDREG systems in place. This Plan will be updated periodically and will remain in effect until rescinded by the OTSG, AMEDD Functional Proponent Agency.

Mission/System Description

MEDREG was developed to assist tactical and medical commanders accomplish the medical mission within the combat theater. MEDREG is an automated, interactive system that will manage combat medical information. TAMMIS MEDREG allows the Medical Regulator to regulate Patients locally within his command or to regulate patients to a higher echelon of care.

Scope

All changes to the MEDREG system to support the transition to the Year 2000 were incorporated in the Nov 1998 Release. The system is being audited for Y2K compliance. The latest version is HKE 04-04 incorporates the changes since the certified release. All changes were tested to insure that there was no adverse impact to the Year 2000 compliance. Any updates required to the system prior to the Year 2000 transition will be evaluated for the impact on this plan and the plan will be updated accordingly.

Background

Y2K Problem. The Year 2000 (Y2K) problem stems from the practice of using two digits instead of four (e.g. “99” vs “1999”) to represent the year, resulting in the inability of computers and devices to interpret Year 2000 dates as greater than 1900 dates. This problem becomes increasingly complex since corrupted data can be perpetuated through interfaces with other information systems. Automated systems such as, MEDREG rely heavily on computers for mission accomplishment. Because of the widespread practice of using only two digits to represent the year in computer databases, software applications, and hardware chips, the potential exists for the failure of automated information systems (AIS) and infrastructure related items on or about 1 January 2000. This potential for failure is referred to as the “Y2K problem”. Y2K related difficulties will arise when date cognizant devices attempt to sort or calculate using the year “00”, not recognizing that the year is actually 2000. The resulting inaccuracies in date-related calculations could generate corrupt results and potentially cause systems to fail. Also, if erroneous data go unrecognized, the problem could be perpetuated

through interfaces (whether fully automatic or “air gapped” such as hand-carried disk or tape) to other systems including systems outside of AMEDD. As if this wasn’t bad enough, many systems have faulty logic that will not recognize the year 2000 as a leap year, leading to the incorrect calculation of the day of the week from 29 February 2000 through the end of the year. Other systems have triggers that are executed based on specific values of date fields, and still others have numeric overflow or rollover problems. The Y2K problem is unique in that our traditional COOP plans and back-up systems may be effected by the same problem(s) as our primary systems - thus rendering them useless. In some cases, the Y2K problem may require a completely different method of accomplishing the mission. The benefits of information technology (IT) have been applied to many aspects of our missions. In many cases, IT allows us to do our jobs better, cheaper, and faster than could be done without it. As the new century approaches, incorrect data generated by date-related processing could have detrimental effects on all information technology (IT) systems. Our challenge is to overcome the potential widespread failure of systems and equipment due to problems associated with processing date information associated with the year-2000. In many instances, Y2K related failures could seriously impair the AMEDD mission. To address this Y2K problem, AMEDD directed development of this COOP to identify potential risks and plans to continue operations when failures occur.

Critical Midnight Crossings

The dates listed below constitute the minimum set of critical dates that have been identified and should be considered in the future when addressing potential year 2000 transition risks:

- 30 Sep 1999 to 1 Oct 1999: For the government calendar, this is the beginning of the fiscal year 2000.
- 31 Dec 1999 to 1 Jan 2000: This is the basic Y2K transition and the one that is most likely to cause a product or process to fail.
- 28 Feb 2000 to 29 Feb 2000: The year 2000 is also a leap year, although some systems may not recognize that. Systems may not perform the leap year calculation properly.
- 29 Feb 2000 to 1 Mar 2000: This time frame must be watched to ensure systems don’t calculate a February 30th.
- 30 Sep 2000 to 1 Oct 2000: This time frame must be watched to ensure systems evaluate the fiscal change over properly.
- 30 Dec 2000 to 1 Jan 2001: This final risk period completes the leap year evaluation by establishing that the system “knows” that the year 2000 has 366 days.

As a minimum precaution, you must ensure that end of day functions have been processed prior to the midnight crossings, a MEDREG and all current daily MEDREG functions are printed in case it becomes necessary to implement the manual mode of operation. These daily functions become the baseline for your manual operations.

Consideration must also be given to limiting the granting of leave, ensuring recall processes are in place and executable, and preposition personnel during these potential critical periods.

Reference Documents

DoD Year 2000 Management Plan, 25 January 1999
DoDD 3026.26 Continuity of Operations Policies and Planning, 26 May 1995
OSD (HA) MHS Year 2000 Contingency and Continuity of Operations Planning Guide, 1 Oct 1998
Contingency Planning Guidance, 1 Oct 1998

Trigger Mechanisms

This COOP will be executed for any serious degradation of the MEDREG system capability related to Y2K failures. Examples of potential hazards are contained in Appendix D. If there are any serious service disruptions affecting mission accomplishment, the affected organization will promptly notify the TAMMIS Customer Support Office (CSO) Help Desk, DSN 421-8533 (Commercial 1-800-927-7675), and provide an assessment of the degradation. Trigger events or system indicators that may require activation of this plan include erratic system results, system degradation, corrupt data, or catastrophic failures. For each of the critical Y2K dates listed above, Patient Systems must check system functions and judge the results of their performance, evaluate actual damage, determine any corrective action required, and notify all effected parties. The Patient Administrator will promptly implement actions to restore mission capability when possible and notify the TAMMIS CSO Help Desk of any mission degradation. Alternatives, in the event of disruption, are identified in Appendices C & D to this plan. For serious disruptions, execution of these alternatives will be at the direction of the program office.

Exit Criteria

Returning to normal operations normally occurs when the AIS project office and/or other organization has repaired the system (or system element) that triggered the contingency operation, affected the repair at the operating site and provided instructions for resuming normal operations. To affect normal operation may typically involve some or all of the following actions:

- Data recovery which may involve reloading the last correct data back-up and recapturing data recorded manually during the contingency operating period and preparing it for data entry.
- Locally testing the AIS (or other system elements) to ensure normal operations have been achieved by the system element repair (directions are provided by the AIS project office should local testing be necessary)

- Assuming normal operations by notifying all parties involved that manual operations have ended and normal automated operations will be begin at a specified and coordinated time.

Roles and Responsibilities

USAMISSA TAMMIS PMO's role is to ensure that users of the MEDREG system have a smooth transition to the new millennium. TAMMIS PMO is responsible for correcting any systemic Y2K problems that may have been overlooked in the Y2K certification. TAMMIS PMO must stay directly involved with the Y2K issue because the AMEDD Patient Systems mission relies heavily on the MEDREG computer information system. Every Patient Administrator must continue to take a direct and active role in the Y2K resolution process, acting decisively and proactively to ensure that their systems, equipment, and forces are mission ready.

Points of Contact

ORGANIZATION	TELEPHONE	NAME & EMAIL
USAMISSA TAMMIS PMO	210-221-1300	MAJ Craig Anderson maj_craig_anderson@smtplink.medcom.amedd.army.mil
Research, Analysis & Maintenance (RAM)	210-829-7541	Juan Luevano juan_luevano@smtplink.medcom.amedd.army.mil
TAMMIS Customer Support Office	210-821-5784	Myrna Pina myrna_pina@smtplink.medcom.amedd.army.mil

Assumptions

The fundamental assumption is that due diligence and professional care have been used in assessing, renovating, and testing MEDREG to ensure year 2000 compliance; however, continuity plans should be developed and tested to address the possibility that failures will still occur because:

- Insufficient time, money, or personnel exist to find and fix all Y2K problems in systems and system interfaces supporting AMEDD operations.
- Some systems may be "infected" with bad date data from another organization's system because it's impossible to ensure that all externally interfaced organizations will have fixed their systems.
- Some problems will occur that are beyond AMEDD control which will impact mission accomplishment.

Coordination Activities

First and foremost is the fact that the MEDREG system has a direct impact on patient care and is the primary reason this system is labeled as mission essential. Any interruption to the system must be immediately evaluated for its impact on providing support to patient care. The commander and health care providers must be advised of any degradation of service so that appropriate measures can be taken.

Actions must be taken to notify organizations responsible for systems that interface with MEDREG and to resolve any Y2K compliance issues. These same organizations must be included in any efforts to resolve system Y2K related degradations, should they occur. The systems that interface are:

- Medical Patient Accounting and Reporting (MEDPAR)
- Defense Medical Regulating Information System (DMRIS)

Review and Update Plan

This COOP will be updated quarterly, beginning 1 Jul 1999. It must remain a “living document” to keep pace with developments in system support requirements.

Contingency and Continuity of Operations Plan Validation

This Contingency and Continuity of Operations Plan must be exercised to ensure it is functional and those action items contained in the plan have been accomplished.

Training

Before conducting any exercise, personnel must be trained on COOP content, exercise objectives, and exercise reporting requirements. The training must be completed before any critical Y2K midnight crossings.

Zero Day Strategies

A zero day strategy involves identifying those actions that will be taken on critical midnight crossings. It also includes troubleshooting/system "health analysis" procedures such as reviewing user screens, validating full system functionality, entering test data and verifying the system performs appropriate data processing functions and produces expected results.

The table below addresses fundamental procedures to follow after any critical midnight crossings. In addition, Appendix E contains detailed manual operating procedures to be used in case the MEDREG system is seriously degraded or drops off line.

Theater Army Medical Management Information System, Programmatic Zero-day Strategies	
Planning Element	Elements of Zero-day Strategy
Staff resource assignments	• Limit leaves for personnel the week before and four weeks after the fiscal and calendar start dates (1 Oct 99 and 1 Jan 2000). • Include similar limited absence clause in written task statements/delivery orders with system developer and support contractor.
General Readiness	• Include in task statement/delivery order for FY99 that the developmental environment will be reserved for repairing and testing Y2K related system failures. • Include language requiring support contractor and vendor to devote key technical personnel to Y2K-related problem analysis and repair.
Coordination with interfacing organizations	• Conduct interfaces testing and verify receipt of scripted data. • Review memorandums of understanding/agreements with DAAS to ensure roles, responsibilities, and resource allocations are in place and clearly understood.
Open ongoing communications	• Review and test lines/methods of communications with the user community the last week of September 1999 and the last week of December 1999. • Validate POC list in mid September. • Begin issuing Y2K bulletins to user community during September 1999. First issues to advise user community of test scenarios, current POC list, review problem reporting procedures, and other topics deemed appropriate. • Use Y2K bulletins and the TAMMIS Web Site to advise user community how best to respond to Y2K incidents. • Develop and publish multiple avenues for communicating with the TAMMIS Project Office.
Project schedules	• For each major problem event (system failure that cannot be corrected with in 72 hours) a task/project name, number, and master schedule will be manifested. • An event schedule will be developed and agreed to by all participants (interfacing organizations, contractors, and vendors), and other interested parties.

Appendix A - Acronyms

AIS	Automated Information System
AMEDD	Army Medical Department
COOP	Continuity of Operations Plan
CP	Contingency Plan
CSO	Customer Support Office
C^o	Consequences of Occurrence
DISA	Defense Information Systems Agency
DMRIS	Defense Medical Regulating Information System
DoD	Department of Defense
DoDD	Department of Defense Directive
DRMO	Defense Redistribution and Marketing Office
IT	Information Technology
MEDPAR	Medical Patient Accounting and Reporting
MEDREG	Medical Regulating
MHS	Military Health System
NOD	Network Operation Division
OASD(C3I)	Office of the Assistance Secretary of Defense (Command, Control, Communications, and Intelligence)
OASD(HA)	Office of the Assistance Secretary of Defense (Health Affairs)
OMB	Office of Management and Budget
OTSG	Office of the Surgeon General
PM	Project or Program Manager

PMO	Program Manager Office
P^o	Probability of Occurrence
RAM	Research, Analysis & Maintenance Inc.
RC	Risk Classification (high, medium, low)
TAMMIS	Theater Army Medical Management Information System
USAMISSA	U.S. Army Medical Information Systems and Services Agency
Y2K	Year 2000

Appendix B – Glossary

Critical Midnight Crossings	A term used to denote certain days when the calendar date changes which is affected by the Millennium change from the 1900s to the year 2000.
Y2K Problem	Problems associated with the change of any date to a year 2000 date.

Appendix C - Systems Contingency Plan

This appendix contains a fundamental systematic approach to dealing with system problems. The subject headings are:

Normal Operating Procedures. This column covers problem resolution procedures in a normal environment.

Risk/Probability of Occurrence/Consequences/Risk Classification. These columns identify contingency hazards or risks that are addressed in the plan. Risk assessment is the first step in preparing the system element of the AIS contingency plan. It is conducted in three stages:

- **Identify risks. The identification, under the system contingency plan, involves the analyses of risks that might inhibit the AIS project managers' ability to identify, report, analyze, repair, test, and distribute system repairs to the user community.**
- **Determine the probability of occurrence (P^o) and consequences of occurrence (C^o). Once a set of risks or hazards is identified, the P^o and C^o are subjectively determined and rated as a low, medium, or high risk.**
- **Determine the risk classification (RC). Risk classification is determined by multiplying P^o and C^o. General rules for arriving at risk classification are contained in the table below.**

Risk Classification Guidelines

P^O	*TIMES*	C^O	*EQUALS*	*RC*
Low	X	Low	=	Low
Low	X	Medium	=	Medium
Low	X	High	=	Medium to High
Medium	X	Low	=	Low
Medium	X	Medium	=	Medium
Medium	X	High	=	High
High	X	Low	=	Low to Medium
High	X	Medium	=	Medium to High
High	X	High	=	High

Contingency Operations Mode. This column addresses procedures to be used in a contingency environment.

MEDREG System-Level AIS Contingency Plan

Normal Operating Procedures	Risk	P^o	C^o	RC	Contingency Operations Mode
Problem Identification					
1. User reports problem by calling local MEDPAR supervisor or system administrator.	Local help desk unable to resolve.	L	H	H	User implements partial/full contingency operating mode (e.g., manually support business process).

2.	User reports problem to CSO.	CSO unable to resolve.	H	H	H	User implements manual operating mode pending problem resolution.
3.	CSO reports problem to AIS Project Manager.	AIS Project Office unable to resolve.	H	L	L	User implements manual operating mode pending problem resolution.
Problem Analyses						
1.	AIS Project staff resolves problem, provides fix guidance to site.	Project staff unable to resolve problem.	L	H	M	Activate contractor/vendor support IAW statements of work/delivery orders.
2.	Determine if problem is caused by hardware, system software, or local/wide area communications.	Failure to identify problem cause by AIS PM.	L	L	L	Implement contract/delivery order to conduct problem analyses. Use vendor developmental environment, as arranged.
Software Repair/Problem Resolution						
1.	AIS Project Office repairs problem, provides fix to user.	Unable to resolve, not an AIS problem	L	L	L	Exercise joint agreements with interfacing organization/project.
2.	AIS Project Office repairs problem, provides fix to user.	Unable to resolve, software problem	L	L	L	Exercise pre-existing written agreements with hardware vendor to repair and distribute/deploy repair.
3.	AIS Project Office repairs problem, provides fix to user.	Unable to resolve, local/wide area communications problem.	L	L	L	Implement agreement(s) with USAMISSA NOD/vendor to resolve problem. Implement agreement to use contractor resources. Implement on-site problem resolution procedures.
4.	AIS Project Office repairs problem, provides fix to user.	Unable to resolve, system SW issue.	L	L	L	Exercise repair agreement(s) with vendor(s) to affect repair.
Software Distribution						
1.	AIS Project Office distributes software fix via U.S. Mail distribution magnetic media.	U.S. Mail too slow to meet distribution requirements.	L	L	L	Express mail option, as appropriate. Validate data recovery procedures during testing, and include instructions for data recovery.
2.	Hardware fix implemented by vendor.	Vendor is overrun with Y2k problems.	L	L	L	Exercise agreement(s) for vendor(s) or alternate sources to conduct on-site repair and implementation.

Appendix D - Continuity of Operations (COOP) Plan

The Continuity of Operations Plan addresses possible failure modes that could impact system operation and mission accomplishment. It focuses more directly on user needs and specific work-around for these failure modes. Subject headings for the plan is:

Process/Function. This identifies a particular function within the system, such as data processing, communication, or information presentation.

Risk/Probability of Occurrence/Consequences/Risk Classification. These columns identify contingency hazards or risks that are addressed in the plan within each Process/Function. Risk assessment is the first step in preparing the system element of the AIS contingency plan. It is conducted in three stages:

- **Identify risks. The identification, under the system contingency plan, involves the analyses of risks that might inhibit the AIS project managers' ability to identify, report, analyze, repair, test, and distribute system repairs to the user community.**
- **Determine the probability of occurrence (P^o) and consequences of occurrence (C^o). Once a set of risks or hazards is identified, the P^o and C^o are subjectively determined and rated as a low, medium, or high risk.**
- **Determine the risk classification (RC). Risk classification is determined by multiplying P^o and C^o. General rules for arriving at risk classification are contained in the table below.**

- **Risk Classification Guidelines**

P^O	TIMES	C^O	EQUALS	RC
Low	X	Low	=	Low
Low	X	Medium	=	Medium
Low	X	High	=	Medium to High
Medium	X	Low	=	Low
Medium	X	Medium	=	Medium
Medium	X	High	=	High
High	X	Low	=	Low to Medium
High	X	Medium	=	Medium to High
High	X	High	=	High

Pre-Contingency Planning. This column addresses things to be done before the contingency to reduce the risk and help in preserving mission capability.

Contingency Execution. This column identifies the procedures to be used if the contingency occurs and your system is impacted. It also focuses on maintaining mission capability.

Post Contingency Recovery. This column establishes procedures for returning systems to an "on-line" status.

Resources. This is a summation of resources required to reduce risk prior to contingencies, execute contingency operations, and recover from contingency operations, including bringing systems back on-line in a normal operating mode. Resources may include such categories as funding, personnel, and equipment.

Continuity of Operations Plan

MEDREG Contingency of Operations Plan						
Process/Function	**Hazard/Risk**	**P^0**	**C^0**	**RC**	**PreContingency Planning**	**Contingency Execution**
MEDREG total system failure	Hardware platform failure	L	L	L	· Maintain current backups · Maintain/print current reports · Provide agencies written notification of alternate operating procedures	· Initiate manual operating procedures · Isolate and fix and/or replac hardware platform if possib · Notify Agencies
	Software failure	L	L	L	· Maintain current backups · Maintain/print current reports · Provide agencies written notification of alternate operating procedures	· Initiate manual operating procedures · Contact contractor for solution
	Power loss	L	L	L	· Maintain current backups · Maintain current reports · Provide agencies written notification of alternate operating procedures	· Initiate manual operating procedures · Notify Agencies · Shut down system before UPS go dead
	Fire	L	L	L	· Maintain current backups Offsite · Maintain current reports	· Operate manually if possibl · Notify command · Notify AIS project office
MEDREG File Transmission	Loss Local Area Network Connection	L	L	L	· Transmit files frequently so there is not a backlog · Provide agencies written notification of alternate operating procedures	· Incoming information from agencies would need to be sent in another format (i.e. mail, fax, email, etc…) · Manually input information · Outgoing information to the agencies would need to be printed and sent via mail or fax. (or possibly email)
	MEDREG working but Agency with problems	L	L	L	· Transmit files frequently so there is not a backlog · Obtain agencies written alternate operating procedures	· Work with that Agency to receive data through anothe process and manually input data to MEDREG · Outgoing information to th agencies would need to be printed and sent via mail or fax. (or possibly email).
Building Utilities (other than power)	Loss of temperature control	L	L	L	· Maintain current backups · Maintain current reports	· Initiate manual operating procedures · Notify Agencies · Shut down system before UPS go dead

Appendix E – Manual Operating Instructions

STP 8-71G15-SM-TG, Soldiers Manual, Patient Administration (Manual Procedures) dated 7 February 1995. This manual states the manual procedures and the method to be used. This manual should be used in conjunction with the Contingency Operations Guidance for Deploying Patient Administrators. The following sections are referenced:

USING PATIENT ADMINISTRATION SYSTEM (Manual)

Contingency Operations Guidance for Deploying Patient Administrators contains information used by Patient Administration in a field environment. The following sections are referenced:

CONTINGENCY OPERATIONS PATIENT ADMINISTRATION (Manual)

TAMMIS SYSTEM ADMINISTRATION

Backup Subsystem

SECTION 1. INTRODUCTION. The "Backup Subsystem" menu item allows you to back up files from the hard disk to secondary media such as tapes or floppy diskettes. Performing regular backups reduces the amount of data lost in case of system failure.

You can use this menu item to back up a specified subsystem, a specified subsystem database, or the entire system. Backups should be done regularly according to a schedule. Besides the scheduled backup, special backups should be done BEFORE installing software updates/releases, repairing database files, or making major changes to the system. Furthermore, backups should also be made AFTER making extensive changes such as entering large amounts of data to the system. The following table describes backup types and their suggested frequencies.

BACKUP TYPE	**BACKUP CONTENTS AND FREQUENCY**
All Sys	Everything currently loaded on the system will be backed up. You should back up the entire system every week.
Subsystem	The specified subsystem and its database will be backed up. You should back up each application and TAMADM biweekly. Also, back up immediately before every software update or database repair.
Subsystem Database	The specified subsystem's database, archive files, and local reports will be backed up. You should back up each subsystem's database daily or once every 12 hours of continuous operation. Do not back up the subsystem database on days you back up the subsystem because the database is included in the subsystem backup.

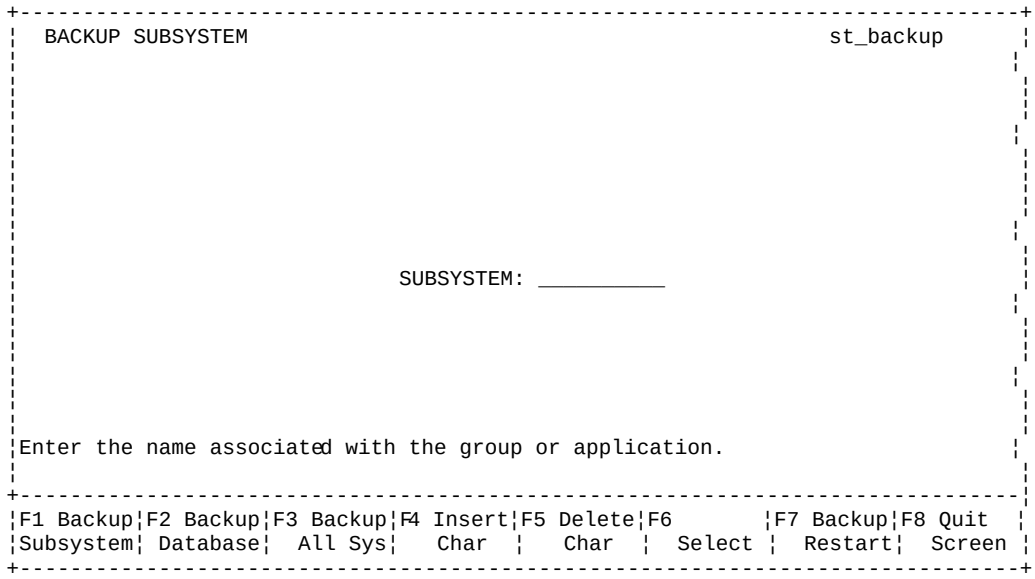
NOTE: The TAMADM database should be backed up after changing passwords or user definitions, adding or deleting a subsystem, or changing TAMMIS communications setups.

You can use either floppy diskette or tape for backups. Tapes are preferred because they can store more information than floppy diskettes. When using any magnetic media, follow these basic guidelines:

- Format floppy diskettes before using them for backup.
- Handle and store all magnetic media with care. Keep them away from heat, humidity, dirt, and magnetism. Remember that electric motors create a magnetic field. Do not set magnetic media on anything electrical, such as the computer terminal.

- Do not fold, staple, or mutilate any magnetic media. Write on a labeled floppy diskette only with a soft-tipped marker.

SECTION 2. PROCEDURES. When you select the "Backup Subsystem" menu item from the Subsystem Maintenance Processes Menu, the system will display the following screen:



The following function keys are available:

- [F1] Backup Subsystem - backs up the entire subsystem including the subsystem database files.
- [F2] Backup Database - backs up only the subsystem's database files.
- [F3] Backup All Sys - backs up the entire computer system.
- [F4] Insert Char - allows you to insert characters in front of the current cursor position.
- [F5] Delete Char - allows you to delete the character at the current cursor position.
- [F6] Select - displays a table of valid names to be entered in the SUBSYSTEM field.
- [F7] Backup Restart - allows you to restart a backup that was previously aborted.
- [F8] Quit Screen - returns to the Subsystem Maintenance Processes Menu.

BEFORE STARTING ANY BACKUP, ENSURE THE FOLLOWING:

- Format ALL media to be used for backups.
- Make sure the selected media is writable. For cartridge tape, the arrow should point away from SAFE (see Figure 4.1-2). For 5¼" floppy diskette, the notch in the upper right hand corner should be open (see Figure 4.1-3). For 3½" floppy diskette, the lower left square window should be closed (see Figure 4.1-4).

Figure 4.1-2. Writable Cartridge Tape

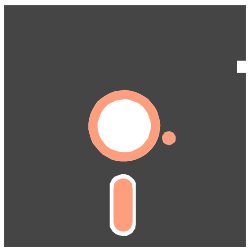


Figure 4.1-3. Writable 5¼" Floppy Diskette

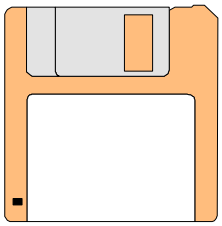


Figure 4.1-4. Writable

- After you have made the backups, make sure the selected media is write-protected. For cartridge tape, the arrow should point toward SAFE (see Figure 4.1-5). For 5¼" floppy diskette, the notch in the upper right hand corner should be covered with tape (see Figure 4.1-6). For 3½" floppy diskette, the lower left square window should be open (see Figure 4.1-7).

Figure 4.1-5. Write-Protected Cartridge Tape

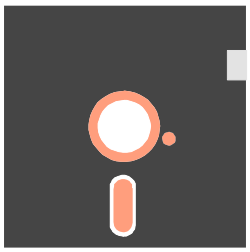


Figure 4.1-6. Write-Protected 5¼" Floppy Diskette

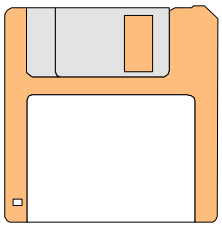


Figure 4.1-7. Write

NOTE: Use only DC 6250 cartridge tapes.

1. HOW TO BACK UP THE ENTIRE SYSTEM.

Press [F3] Backup All Sys. The system will place "All Sys" in the SUBSYSTEM field. The system will ask if you wish to view the list of files as they are being copied to the media. Type **Y** and press [RETURN] if you want the system to display the names of the files across the screen during the copy process. The system will then prompt you for the media type to be used for the backup by displaying the following message prompt on the message line of the screen:

Indicate type of media to be used (C - Cartridge, F - Floppy):

Type **C** for cartridge tape or **F** for floppy diskette and press [RETURN]. If you entered "F," the system will prompt you for the diskette type as follows:

Select diskette size and density

3½ Double Density (720k) = 3d
3½ High Density (1.4m) = 3h
5¼ Double Density (360k) = 5d
5¼ High Density (1.2m) = 5h
Quit = q

Enter choice (3d, 3h, 5d, 5h, q):

Enter your choice and press [RETURN].

The system will calculate the number of volumes needed for the backup and display the information on the screen similar to the following:

Blocksize = 65536

Device to be used for copy
/dev/tape

Number of volumes needed

1 volumes needed

Please label this volume:
system
Volume: 1 of 1
Date archived: Wed May 25 16:56:27 1994
From system: W00004!/

Please insert volume 1, then press [RETURN] (To Quit type "q")

Label the selected media according to the label information provided on the screen (see above for example). Insert the media into the appropriate drive; then press [RETURN].

If this is a multi-volume backup, the system will again display messages telling you how to label the next volume and instructing you to insert the media. Label and insert the tapes or floppy diskettes until the backup ends. When the final volume required for the backup has been completed, the system will display messages similar to the following:

733334784 bytes written.
Finished copying files onto /dev/tape
Please hit return to continue:

Press [RETURN] to return to the menu.

2. HOW TO BACK UP A SUBSYSTEM.

Enter the subsystem name in the SUBSYSTEM field and press [F1] Backup Subsystem.

NOTE: You can only backup TAMADM using either [F2] Backup Database or [F3] Backup All Sys.

If you entered an invalid name, the following message will be displayed on the message line:

ERROR: Your entry does not exist in file of valid entries. Check for Select.

Press [F6] Select to bring up the select table of valid entries. Highlight the desired name and press [F1]. The system will place the subsystem name you selected in the SUBSYSTEM field.

If you entered a valid name and pressed [F1] Backup Subsystem, the system will ask if you wish to view the list of files as they are being copied to the media. Type **Y** and press [RETURN] if you want the system to display the names of the files across the screen during the copy process. The system will then prompt you for the media type to be used for the backup with the following message:

Indicate type of media to be used (C - Cartridge, F - Floppy):

Type **C** for cartridge tape or **F** for floppy diskette and press [RETURN]. If you entered "F," the system will prompt you for the diskette type as follows:

Select diskette size and density

3½ Double Density (720k)	**= 3d**
3½ High Density (1.4m)	**= 3h**
5¼ Double Density (360k)	**= 5d**
5¼ High Density (1.2m)	**= 5h**
Quit	**= q**

Enter choice (3d, 3h, 5d, 5h, q):

Enter your choice and press [RETURN].

The system will calculate the number of volumes needed for the backup and display the information on the screen similar to the following:

Blocksize = 65536

Device to be used for copy
/dev/tape

Number of volumes needed

1 volumes needed

Please label this volume:
medreg subsystem
Volume: 1 of 1
Date archived: Wed May 25 16:56:27 1994
From system: W00004!/

Please insert volume 1, then press [RETURN] (To Quit type "q")

Label the selected media according to the label information provided on the screen (see above for example). Insert the media into the appropriate drive; then press [RETURN].

If this is a multi-volume backup, the system will again display the messages telling you how to label the next volume and instructing you to insert it. Label and insert the tapes or floppy diskettes until the backup ends. When the final volume required for the backup have been completed, the system will display messages similar to the following:

17104896 bytes written.
Finished copying files onto /dev/tape
Please hit return to continue:

Press [RETURN] to return to the menu.

3. HOW TO BACK UP THE SUBSYSTEM DATABASE.

Enter the subsystem name in the SUBSYSTEM field and press [F2] Backup Database.

If you entered an invalid name, the following message will be displayed on the message line:

ERROR: Your entry does not exist in file of valid entries. Check for Select.

Press [F6] Select to bring up the select table of valid entries. Highlight the desired name and press [F1]. The system will place the subsystem name you selected in the SUBSYSTEM field.

If you entered a valid name and pressed [F2] Backup Database, the system will ask if you wish to view the list of files as they are being copied to the media. Type **Y** and press [RETURN] if you want the system to display the names of the files across the screen during the copy process. The system will then prompt you for the media type to be used for the backup with the following message prompt:

Indicate type of media to be used (C - Cartridge, F - Floppy):

Type **C** for cartridge tape or **F** for floppy diskette and press [RETURN]. If you entered "F," the system will prompt you for the diskette type as follows:

Select diskette size and density

3½ Double Density (720k) = 3d
3½ High Density (1.4m) = 3h
5¼ Double Density (360k) = 5d
5¼ High Density (1.2m) = 5h
Quit = q

Enter choice (3d, 3h, 5d, 5h, q):

Enter your choice and press [RETURN].

The system will calculate the number of volumes needed for the backup and display the information on the screen similar to the following:

Blocksize = 65536

Device to be used for copy
/dev/tape

Number of volumes needed

1 volumes needed

Please label this volume:
medreg database
Volume: 1 of 1
Date archived: Wed May 25 16:56:27 1994
From system: W00004!/

Please insert volume 1, then press [RETURN] (To Quit type "q")

Label the selected media according to the label information provided on the screen (see above for example). Insert the media into the appropriate drive; then press [RETURN].

If this is a multi-volume backup, the system will again display the messages telling you how to label the next volume and instructing you to insert it. Label and insert the tapes or floppy diskettes until the backup ends. When the final volume required for the backup have been completed, the system will display messages similar to the following:

4551009 bytes written.
Finished copying files onto /dev/tape
Please hit return to continue:

Press [RETURN] to return to the menu.

4. HOW TO RESTART A BACKUP.

If a backup failed or if you aborted a backup, you can restart by pressing [F7] Backup Restart.

If you did not previously abort the backup and you attempt to restart, the system will display the following message:

Restart of backup cannot be done. The backup file list does not exist.

You will then be returned to the SUBSYSTEM field.

If you previously aborted the backup, the system will display the following message prompt:

Which volume number do you wish to restart on? (Hit return for default)

Type the volume number and press [RETURN] or press [RETURN] to continue the backup before you aborted the procedure. The system will prompt you for the media type to be used for the backup by displaying the following message:

Indicate type of media to be used (C - Cartridge, F - Floppy):

Type **C** for cartridge tape or **F** for floppy diskette and press [RETURN]. If you entered "F," the system will prompt you for the diskette size as follows:

Select diskette size and density

3½ Double Density (720k) = 3d
3½ High Density (1.4m) = 3h
5¼ Double Density (360k) = 5d
5¼ High Density (1.2m) = 5h
Quit = q

Enter choice (3d, 3h, 5d, 5h, q):

Enter your choice and press [RETURN].

If you entered the correct restart volume number or you pressed [RETURN], the system will display messages similar to the following:

Blocksize = 65536

Device to be used for copy
/dev/rdsk/f0q18dt

This volume has been aborted.
Will attempt to write this same volume again.
Please label this volume:
Volume 2 of 13
Date archived: Fri Jun 10 17:25:04 1994
From system: W00004!/

Please insert volume 2, then press [RETURN] (To Quit type "q")

Insert the appropriate media into the drive and press [RETURN] to restart the backup or **q** to quit.

If you attempt to restart on a volume that is different from the one aborted, the system will display a warning message similar to the following (the blanks will be replaced with a volume number):

The user-specified volume number _ does NOT match the previously
failed volume number _ .

If you insist on restarting that volume enter the media type, insert the selected media into the appropriate drive and press [RETURN] to restart the backup.

5. SCHEDULING LOG.

To help you follow proper backup procedures, the following form is suggested to schedule and record your system backups.

Backup Schedule					
	Day 1	Day 2	Day 3	Day 4	Week
Date/Initials Type of Backup Volume #					
Date/Initials Type of Backup Volume #					
Date/Initials Type of Backup Volume #					
Date/Initials Type of Backup Volume #					
Date/Initials Type of Backup Volume #					
Date/Initials Type of Backup Volume #					
Date/Initials Type of Backup Volume #					
Date/Initials Type of Backup Volume #					

6. ROTATION OF BACKUP MEDIA.

Each backup creates a set of volumes. Remember that each floppy diskette or tape is a volume. The number in the set depends on the number of volumes required for the backup. Use a new set of backup media each day. DO NOT reuse the backup media until the backup data is obsolete (that is, they no longer have any recovery value).

NOTE: Make certain that you re-label each tape/floppy diskette when you rotate the backup sets.

- Daily Backups — A different set of media will be used to back up the subsystem database for each of the four days; all sets will be reused each week. Rotate the media sequentially by date when reusing them so that you always reuse the oldest set (for example, on Day 1 you will use the set of backup tapes from Day 1 of the previous week.)

- Biweekly Backups — A different set of media will be used for biweekly backups of the subsystem on Day 2 and Day 4. Always rotate the backup media by reusing the oldest set first.

- Weekly Backups — A different set of media will be used for weekly backups of the entire system on Day 5. Always rotate the backup media by reusing the oldest set first.

Press [F8] Quit Screen when you have finished making backups. The system will return to the Subsystem Maintenance Processes Menu.

NOTE: Your backup media will wear out over time. To ensure reliable backups, replace daily backup media once a month, and replace weekly backup media once every six months. Use new media for replacements.

TAMMIS SYSTEM ADMINISTRATION

Restore Subsystem

SECTION 1. INTRODUCTION. The "Restore Subsystem" menu item allows you to restore all files that were backed up on tape(s) or floppy diskette(s) to the hard disk. Use this menu item to recover from problems caused by hardware or system failure.

CAUTION: Do not restore the subsystem while subsystem users are logged on. Before attempting to restore a subsystem, ensure that all subsystem users are logged off. Execute TAMMIS System Administration menu entry 4.2 "TAMMIS Subsystem Shutdown" before attempting to restore the entire system to ensure that ALL users are logged off.

SECTION 2. PROCEDURES. Use the following procedure to recover a subsystem, a subsystem database, or the entire system. Use only backups made after a software installation or database repair to avoid corruption.

When you select the "Restore Subsystem" menu item from the Subsystem Maintenance Processes Menu, the system will ask if you wish to view the list of files as they are being copied from the media. Type **Y** and press [RETURN] if you want the system to display the names of the files across the screen during the copy process. The system will then prompt you for the media type with the following message:

Indicate type of media to be used (C - Cartridge, F - Floppy):

Type **C** if the backup is on cartridge tape or type **F** if it is on floppy diskette. If you entered "F," the system will prompt you for the diskette type as follows:

Select diskette size and density

3½ Double Density (720k) = 3d
3½ High Density (1.4m) = 3h
5¼ Double Density (360k) = 5d
5¼ High Density (1.2m) = 5h
Quit = q

Enter choice (3d, 3h, 5d, 5h, q):

Enter your choice and press [RETURN].

The system will prompt you for the following:

Please enter the restart volume number or [RETURN] to restore entire backup:

- If you pressed [RETURN], the following message will appear:

  Please insert volume 1, then press [RETURN] (To Quit type "q")

- If you entered "1," the following messages will appear:

  You are restarting with volume #1

  Volume 1 restart is treated as a new recovery,
  Please insert volume 1, then press [RETURN] (To Quit type "q")

- If you restart from a previously interrupted recovery, enter the volume number when the interruption occurred and press [RETURN]. The system will display the following messages (the blanks will be replaced with a volume number):

  You are restarting with volume #__
  Please insert volume 1, then press [RETURN] (To Quit type "q")

In any case, insert volume 1 into the drive, wait until the light is turned off, and then press [RETURN]. Depending on the backup media used, the system will display a message similar to one of the following messages:

You are about to do a full-system recovery.

To continue, press [RETURN]. To Quit, type "q".

or

You are about to recover _____ _____.

To continue, press [RETURN]. To Quit, type "q".

Press [RETURN] to begin the recovery or type **q** to quit.

NOTE: In the actual messages, the blanks will be completed with the name of the backup media (for example, medreg subsystem, medreg database).

If the backup includes more than one volume, the system will display a message instructing you to load another volume when it has finished restoring the last volume. The message will be similar to the following (with the blanks replaced with a volume number):

Please insert volume ____, then press [RETURN]. (To Quit type "q")

Insert the correct volume into the drive, wait until the light is turned off, and press [RETURN]. Continue until the recovery ends.

When the system completes the recovery, the following message is displayed:

Recovery completed. Please hit return to continue:

Press [RETURN] to go back to the Subsystem Maintenance Processes Menu.

If you are performing a full-system recovery, execute Menu Item 4.1, "Complete System Shutdown," following the instructions in TAMMIS System Administration User Guide 4, "System Shutdown/Startup".

NOTE: If you shut down the TAMMIS system, execute TAMMIS System Administration menu entry 4.3, "TAMMIS System Startup", to start up the TAMMIS system.

At this time, the users may log onto the system.

NOTE: You may get the following error messages when starting recovery:

Cannot identify backup type.
Backup area will not be cleaned before restoring.
To continue, press [RETURN]. To Quit, type "q".

This means that you have an old backup tape or one that was not created with the TAMMIS System Administration menu system. This is not a normal situation! If you allow this recovery to continue, you can destroy data and programs on your system.

WARNING: Do not proceed with the recovery unless you are absolutely certain that it is the only way to recover the data on the media and the media does not contain data you do not want recovered!

If there is any doubt about recovering from an unidentifiable tape, *DO NOT DO IT*. Type **q** to quit. Otherwise, verify that the recovery you are about to do is the one you intended then press [RETURN] to perform the recovery.